ON EISENSTEIN IDEALS AND THE CUSPIDAL GROUP OF $J_0(N)$

HWAJONG YOO

ABSTRACT. Let $\mathcal{C}_N$ be the cuspidal subgroup of the Jacobian $J_0(N)$ for a square-free integer $N > 6$. For any Eisenstein maximal ideal $\mathfrak{m}$ of the Hecke ring of level N, we show that $\mathcal{C}_N[\mathfrak{m}] \neq 0$. To prove this, we calculate the index of an Eisenstein ideal $\mathcal{I}$ contained in $\mathfrak{m}$ by computing the order of the cuspidal divisor annihilated by $\mathcal{I}$.

CONTENTS

1. INTRODUCTION

Let N be a square-free integer greater than 6 and let $X_0(N)$ denote the modular curve over $\mathbb{Q}$ associated to $\Gamma_0(N)$, the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of upper triangular matrices modulo N. There is the Hecke ring $\mathbb{T} := \mathbb{T}(N)$ of level N, which is the subring of the endomorphism ring of the Jacobian variety $J_0(N) := \mathrm{Pic}^0(X_0(N))$ of $X_0(N)$ generated by the Hecke operators T_n for all $n \geq 1$. A maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ is called *Eisenstein* if the two dimensional semisimple representation $\rho_{\mathfrak{m}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{T}/\mathfrak{m}$ attached to $\mathfrak{m}$ is reducible, or equivalently $\mathfrak{m}$ contains the ideal

$$\mathcal{I}_0(N) := (T_r - r - 1 \ : \ \text{for primes } r \nmid N).$$

Let $\mathcal{C}_N$ be *the cuspidal group* of $J_0(N)$ generated by degree 0 cuspidal divisors, which is finite by Manin and Drinfeld [11, 4].

Ribet conjectured that all Eisenstein maximal ideals are "cuspidal". In other words, $\mathcal{C}_N[\mathfrak{m}] \neq 0$ for any Eisenstein maximal ideal $\mathfrak{m}$. There were many evidences of this conjecture. In particular, special cases were already known (cf. [21, §3]). In this paper, we prove his conjecture.

Theorem 1.1 (Main theorem)**.** *Let $\mathfrak{m}$ be an Eisenstein maximal ideal of $\mathbb{T}$. Then $\mathcal{C}_N[\mathfrak{m}] \neq 0$.*

To prove this theorem, we classify all possible Eisenstein maximal ideals in §2. From now on, we denote by U_p the p^{th} Hecke operator $T_p \in \mathbb{T}$ when $p \mid N$.

Proposition 1.2. *Let $\mathfrak{m}$ be an Eisenstein maximal ideal of $\mathbb{T}$. Then, it contains*

$$I_{M,N} := (U_p - 1,\ U_q - q,\ \mathcal{I}_0(N) \ : \ \textit{for primes } p \mid M \ \textit{ and } q \mid N/M)$$

for some divisor M of N such that $M \neq 1$.

2010 *Mathematics Subject Classification.* 11G18, 14G35.
Key words and phrases. Eisenstein ideals, Cuspidal groups.

In §3, we study basic properties of the cuspidal group $\mathcal{C}_N$ of $J_0(N)$. In particular, we explicitly compute the order of the cuspidal divisor $C_{M,N}$, which is the equivalence class of $\sum_{d|M}(-1)^{\omega(d)}P_d$, where $\omega(d)$ is the number of distinct prime divisors of d and P_d is the cusp of $X_0(N)$ corresponding to $1/d \in \mathbb{P}^1(\mathbb{Q})$.

Theorem 1.3. *The order of $C_{M,N}$ is equal to the numerator of $\frac{\varphi(N)\psi(N/M)}{24} \times h$, where h is either 1 or 2. Moreover, $h = 2$ if and only if one of the following holds:*

(1) *$N = M$ and M is a prime such that $M \equiv 1 \pmod 8$;*
(2) *$N = 2M$ and M is a prime such that $M \equiv 1 \pmod 8$.*

(See Notation 1.1 for the definition of $\varphi(N)$ and $\psi(N)$.) This theorem generalizes the works by Ogg [14, 15] and Chua-Ling [1] to the case where $\omega(N) \geq 3$. In §4, we introduce Eisenstein series and compute their residues at various cusps. With these computations, we can prove the following theorem in §5.

Theorem 1.4. *If $M \neq N$ and N/M is odd, then the index of $I_{M,N}$ is equal to the order of $C_{M,N}$. Moreover, if $M = N$ or N/M is even, then the index of $I_{M,N}$ is equal to the order of $C_{M,N}$ up to powers of 2.*

Finally, combining all the results above, we prove our main theorem in §6.

Acknowledgements. We are grateful to Ken Ribet for suggesting the problem and his advice during the preparation of this work. We thank the anonymous referee for careful reading and a number of suggestions and corrections to improve the paper.

1.1. **Notation.** For a square-free integer $N = \prod_{i=1}^n p_i$, we define the following quantities:

$$\omega(N) := n = \text{ the number of distinct prime divisors of } N;$$

$$\varphi(N) := \prod_{i=1}^n (p_i - 1) \quad \text{and} \quad \psi(N) := \prod_{i=1}^n (p_i + 1).$$

For any rational number $x = a/b$, we denote by $\mathrm{num}(x)$ the numerator of x, i.e.,

$$\mathrm{num}(x) := \frac{a}{(a,b)}.$$

For a prime divisor p of N, there is the degeneracy map $\gamma_p : J_0(N/p) \times J_0(N/p) \to J_0(N)$ (cf. [16, §3]). The image of γ_p is called the *p-old subvariety* of $J_0(N)$ and is denoted by $J_0(N)_{p\text{-old}}$. The quotient of $J_0(N)$ by $J_0(N)_{p\text{-old}}$ is called the *p-new quotient* and is denoted by $J_0(N)^{p\text{-new}}$. Note that $J_0(N)_{p\text{-old}}$ is stable under the action of Hecke operators and γ_p is Hecke-equivariant. Accordingly, the image of $\mathbb{T}(N)$ in $\mathrm{End}(J_0(N)_{p\text{-old}})$ (resp. $\mathrm{End}(J_0(N)^{p\text{-new}})$) is called the *$p$-old* (resp. *$p$-new*) *quotient* of $\mathbb{T}(N)$ and is denoted by $\mathbb{T}(N)^{p\text{-old}}$ (resp. $\mathbb{T}(N)^{p\text{-new}}$). A maximal ideal $\mathfrak{m}$ of $\mathbb{T}(N)$ is called *p-old* (resp. *p-new*) if its image in $\mathbb{T}(N)^{p\text{-old}}$ (resp. $\mathbb{T}(N)^{p\text{-new}}$) is still maximal. Note that if a maximal ideal $\mathfrak{m}$ of $\mathbb{T}(N)$ is p-old, then there is a maximal ideal $\mathfrak{n}$ of $\mathbb{T}(N/p)$ corresponding to $\mathfrak{m}$ (cf. [17, §7]).

For a prime divisor p of N, we denote by w_p the Atkin-Lehner operator (with respect to p) acting on $J_0(N)$ (and the space of modular forms of level N). (For more detail, see [13, §1].)

For a prime p, we denote by Frob_p an arithmetic Frobenius element for p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

2. Eisenstein ideals

From now on, we denote by N a square-free integer greater than 6 and let $\mathbb{T} := \mathbb{T}(N)$ be the Hecke ring of level N. A maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ is called *Eisenstein* if the two dimensional semisimple representation $\rho_{\mathfrak{m}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{T}/\mathfrak{m}$ attached to $\mathfrak{m}$ is reducible, or equivalently $\mathfrak{m}$ contains the ideal $\mathcal{I}_0(N) := (T_r - r - 1 \,:\, \text{for primes } r \nmid N)$. (For the existence of $\rho_{\mathfrak{m}}$, see [17, Proposition 5.1].)

Let us remark briefly why these two definitions are equivalent. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ containing ℓ. If $\rho_{\mathfrak{m}}$ is reducible, then $\rho_{\mathfrak{m}} \simeq \mathbb{1} \oplus \chi_\ell$, where $\mathbb{1}$ is the trivial character and χ_ℓ is the mod ℓ cyclotomic character, by Ribet [22, Proposition 2.1]. Therefore for a prime r not dividing ℓN, we have

$$T_r \pmod{\mathfrak{m}} = \mathrm{trace}(\rho_{\mathfrak{m}}(\mathrm{Frob}_r)) = 1 + r$$

and hence $T_r - r - 1 \in \mathfrak{m}$. For $r = \ell$, we get $T_\ell \equiv 1 + \ell \equiv 1 \pmod{\mathfrak{m}}$ by Ribet [18, Lemma 1.1]. (This lemma basically follows from the result by Deligne [5, Theorem 2.5] and this is also true even when ℓ divides N.) Conversely, if $\mathfrak{m}$ contains $\mathcal{I}_0(N)$, then $\rho_\mathfrak{m} \simeq \mathbb{1} \oplus \chi_\ell$ by the Chebotarev and the Brauer-Nesbitt theorems.

To classify all Eisenstein maximal ideals, we need to understand the image of U_p in the residue fields for any prime divisor p of N.

Lemma 2.1. *Let $\mathfrak{m}$ be an Eisenstein maximal ideal of $\mathbb{T}$. Let p be a prime divisor of N and $U_p - \epsilon(p) \in \mathfrak{m}$. Then, $\epsilon(p)$ is either 1 or p modulo $\mathfrak{m}$.*

Proof. Assume that $\mathfrak{m}$ is p-old. Then $\mathfrak{m}$ can be regarded as a maximal ideal of $\mathbb{T}^{p\text{-old}}$. Let R be the common subring of the Hecke ring $\mathbb{T}(N/p)$ of level N/p and $\mathbb{T}^{p\text{-old}}$, which is generated by all T_n with $p \nmid n$. Let $\mathfrak{n}$ be the corresponding maximal ideal of $\mathbb{T}(N/p)$ to $\mathfrak{m}$ and T_p be the p^{th} Hecke operator in $\mathbb{T}(N/p)$. Then, we get

$$\mathbb{T}(N/p) = R[T_p] \quad \text{and} \quad \mathbb{T}(N)^{p\text{-old}} = R[U_p]$$

[17, §7] and $\mathbb{T}/\mathfrak{m} \simeq \mathbb{T}(N/p)/\mathfrak{n}$. Two operators T_p and U_p are connected by the quadratic equation $U_p^2 - T_pU_p + p = 0$ (*loc. cit.*). Note that $T_p - p - 1 \in \mathfrak{n}$ because $\mathfrak{n}$ is Eisenstein as well. Therefore over the ring $\mathbb{T}/\mathfrak{m} \simeq \mathbb{T}(N/p)/\mathfrak{n}$, we get $U_p^2 - (p+1)U_p + p = (U_p - 1)(U_p - p) = 0$ and hence either $\epsilon(p) \equiv 1$ or $p \pmod{\mathfrak{m}}$.

Assume that $\mathfrak{m}$ is p-new. Then $\epsilon(p) = \pm 1$. Therefore it suffices to show that $\epsilon(p) \equiv 1$ or $p \pmod{\mathfrak{m}}$ when $\epsilon(p) = -1$. Let ℓ be the residue characteristic of $\mathfrak{m}$. If $\ell = 2$, then there is nothing to prove because $1 \equiv -1 \pmod{\mathfrak{m}}$. If $\ell = p$, then $U_p \equiv 1 \pmod{\mathfrak{m}}$ by Ribet [18, Lemma 1.1]. Therefore we assume that $\ell \geq 3$ and $\ell \neq p$. On the one hand, we have $\rho_\mathfrak{m} \simeq \mathbb{1} \oplus \chi_\ell$. On the other hand, the semisimplification of the restriction of $\rho_\mathfrak{m}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is isomorphic to $\epsilon \oplus \epsilon\chi_\ell$, where ϵ is the unramified quadratic character with $\epsilon(\mathrm{Frob}_p) = \epsilon(p)$ because $\mathfrak{m}$ is p-new (cf. [2, Theorem 3.1.(e)]). Since $\epsilon(p) = -1$, we get $p \equiv -1 \pmod{\ell}$ and hence $\epsilon(p) \equiv p \pmod{\mathfrak{m}}$. □

Let $\mathfrak{m}$ be an Eisenstein maximal ideal of $\mathbb{T}$ containing ℓ. Then, it contains

$$I_{M,N} := (U_p - 1,\ U_q - q,\ \mathcal{I}_0(N)\ :\ \text{for primes } p \mid M \text{ and } q \mid N/M) \subseteq \mathbb{T}$$

for some divisor M of N by the previous lemma. If $q \equiv 1 \pmod{\ell}$ for a prime divisor q of N/M, then $\mathfrak{m} = (\ell,\ I_{M,N}) = (\ell,\ I_{M\times q,N})$. Therefore when we denote by $\mathfrak{m} := (\ell,\ I_{M,N})$ for some divisor M of N, we always assume that $q \not\equiv 1 \pmod{\ell}$ for all prime divisors q of N/M. Hence if $\ell = 2$, then either $\mathfrak{m} := (\ell,\ I_{N,N})$ or $\mathfrak{m} := (\ell,\ I_{N/2,N})$. If $\ell \geq 3$, $\mathfrak{m} := (\ell,\ I_{1,N})$ cannot be maximal by Proposition 5.5. Therefore from now on, we always assume that $M \neq 1$.

3. The cuspidal group

As before, let N denote a square-free integer and let $M \neq 1$ denote a divisor of N. For a divisor d of N, we denote by P_d the cusp corresponding to $1/d$ in $\mathbb{P}^1(\mathbb{Q})$. (Thus, the cusp ∞ is denoted by P_N.) We denote by $C_{M,N}$ the equivalence class of a cuspidal divisor $\sum_{d|M}(-1)^{\omega(d)}P_d$. Note that $I_{M,N}$ annihilates $C_{M,N}$ [21, Proposition 2.13]. To compute the order of $C_{M,N}$, we use the method of Ling [10, §2].

Theorem 3.1. *The order of $C_{M,N}$ is equal to*

$$\mathrm{num}\left(\frac{\varphi(N)\psi(N/M)}{24}\right) \times h,$$

where h is either 1 or 2. Moreover, $h = 2$ if and only if one of the following holds:

1. *$N = M$ and M is a prime such that $M \equiv 1 \pmod 8$;*
2. *$N = 2M$ and M is a prime such that $M \equiv 1 \pmod 8$.*

Remark 3.2. The size of the set $\mathcal{C}_N$ is computed by Takagi [19]. Recently, Harder discussed the more general question of giving denominators of Eisenstein cohomology classes. The order of a cuspidal divisor is a special case of such a denominator and some cases were computed by a slightly different method from the one used here [7, §2].

Before starting to prove this theorem, we define some notations and provide lemmas.

Let $N = \prod_{i=1}^n p_i$. We denote by $\mathcal{S}$ the set of divisors of N. Let $s := 2^n = \#\mathcal{S}$.

(1) For $a \in \mathcal{S}$, we denote by
$$a = (a_1,\, a_2, \cdots, a_n),$$
where $a_i = 0$ if $(p_i,\, a) = 1$; and $a_i = 1$ otherwise. For instance, $1 = (0,\, 0, \cdots, 0)$ and $N = (1,\, 1, \cdots, 1)$.

(2) We define the total ordering on $\mathcal{S}$ as follows.
Let $a, b \in \mathcal{S}$ and $a \neq b$.
- If $\omega(a) < \omega(b)$, then $a < b$. In particular, $1 < a < N$ for $a \in \mathcal{S} \setminus \{1, N\}$.
- If $\omega(a) = \omega(b)$, then we use the anti-lexicographic order. In other words, $a < b$ if $a_i = b_i$ for all $i < t$ and $a_t > b_t$.

(3) We define the box addition $\boxplus$ on $\mathcal{S}$ as follows.
$$a \boxplus b := (c_1,\, c_2, \cdots, c_n),$$
where $c_i \equiv a_i + b_i + 1 \pmod 2$ and $c_i \in \{0, 1\}$. For instance, $p_1 \boxplus p_1 = N$ and $1 \boxplus a = N/a$.

(4) Finally, we define the sign on $\mathcal{S}$ as follows.
$$\operatorname{sgn}(a) := (-1)^{s(a)},$$
where $s(a) = \omega(N) - \omega(a)$. For example, $\operatorname{sgn}(N) = 1$ and $\operatorname{sgn}(1) = (-1)^n$.

We denote by $\mathcal{S} = \{d_1,\, d_2,\, \dots,\, d_s\}$, where $d_i < d_j$ if $i < j$. For instance, $d_1 = 1$, $d_2 = p_1$ and $d_s = N$. Note that $d_i \times d_{s+1-i} = N$ for any i.

For ease of notation, we denote by d_{ij} the box sum $d_i \boxplus d_j$.

Lemma 3.3. *We have the following properties of* $\boxplus$.

(1) $d_{ij} = d_{ji} = d_{s+1-i} \boxplus d_{s+1-j}$.
(2) $d_{i1} = N/d_i = d_{s+1-i}$.
(3) $\mathcal{S} = \{d \boxplus d_1,\, d \boxplus d_2,\, \dots,\, d \boxplus d_s\}$ *for any* $d = d_i$.
(4) $\operatorname{sgn}(d_{ij}) = \operatorname{sgn}(d_i) \times \operatorname{sgn}(d_j)$.
(5) *Assume that* $i \neq j$ *and* d_{ij} *is not divisible by* p_n. *Then, for any* d_k *such that* d_{kj} *is not divisible by* p_n, *we get*
$$d_{ik} \times d_{kj} = d_{ir(k)} \times d_{r(k)j},$$
where $r(k)$ *is the unique integer between* 1 *and* s *such that* $d_{r(k)j} = p_n \cdot d_{kj}$.

Proof. The first, second, third and fourth assertions easily follow from the definition.

Assume that $i \neq j$. Then $d_{ij} \neq N$ and there is a prime divisor of N/d_{ij}. Assume that d_{ij} is not divisible by p_n. Let k be an integer such that d_{kj} is not divisible by p_n. Then, we denote by
$$d_i = (a_1, \cdots, a_n) \quad \text{and} \quad d_j = (b_1, \cdots, b_n);$$
$$d_k = (c_1, \cdots, c_n) \quad \text{and} \quad d_{r(k)} = (e_1, \cdots, e_n).$$

By abuse of notation, we denote by $d_{ik} \times d_{kj} = (x_1,\, x_2, \cdots, x_n)$ and $d_{ir(k)} \times d_{r(k)j} = (y_1,\, y_2, \cdots, y_n)$, where $0 \leq x_t,\; y_t \leq 2$. Thus, $d_{ik} \times d_{kj} = \prod_{t=1}^s p_t^{x_t}$. It suffices to show that $x_t = y_t$ for all t.

- Assume that $t \neq n$. From the definition of $d_{r(k)}$, we get $c_t = e_t$. Therefore $x_t = y_t$.
- Since d_{ij} and d_{kj} is not divisible by p_n, we get $a_n + b_n = 1 = c_n + b_n$. Therefore $a_n = c_n$. Since $d_{r(k)j}$ is divisible by p_n, we get $e_n + b_n + 1 \equiv 1 \pmod 2$. Therefore $x_n = y_n = 1$.

$\square$

From now on, we follow the notations in [10, §2]. In our case, the $s \times s$ matrix Λ on page 35 of *op. cit.* is of the form
$$\Lambda_{ij} = \frac{1}{24} a_N(d_i,\, d_j),$$

where

$$a_N(a,\, b) := \frac{N}{(a,\, N/a)} \frac{(a,\, b)^2}{ab}.$$

For examples, $a_N(1,\, p) = N/p$ and $a_N(N,\, p) = p$.

Lemma 3.4. *We get*

$$24 \times \Lambda_{ij} = d_i \boxplus d_j = d_{ij} \in \mathcal{S}.$$

Proof. This is clear from the definition. □

Lemma 3.5. *Let $A := (\mathrm{sgn}(d_{ij}) \times (d_{ij}))_{1 \leq i,\, j \leq s}$ be a $s \times s$ matrix. Then, $A = \frac{\varphi(N)\psi(N)}{24} \times \Lambda^{-1}$.*

Proof. We compute $B := 24 \times \Lambda \times A$.

- Assume that $i = j$. Then, we have

$$B_{ii} = \sum_{j=1}^{s} \mathrm{sgn}(d_{ij}) \times (d_{ij})^2 = \sum_{k=1}^{s} \mathrm{sgn}(d_k) \times d_k^2 = \prod_{k=1}^{n} (p_k^2 - 1) = \varphi(N)\psi(N)$$

  because $\{d_{ij} \;:\; 1 \leq j \leq s\} = \mathcal{S}$ by Lemma 3.3 (3).
- Assume that $i \neq j$. Then, $d_{ij} \neq N$. Let q be a prime divisor of N/d_{ij}. We denote by $\mathcal{T}_j$ the subset of $\mathcal{S}$ such that

$$\mathcal{T}_j := \{d_k \in \mathcal{S} \;:\; (q,\, d_{kj}) = 1\}.$$

  Then the size of $\mathcal{T}_j$ is $s/2$. For each element $d_k \in \mathcal{T}_j$, we can find $d_{r(k)} \in \mathcal{S}$ such that $d_{r(k)j} = q \cdot d_{kj}$ by Lemma 3.3 (3). Moreover $\mathcal{T}_j{}^c = \{d_{r(k)} \;:\; d_k \in \mathcal{T}_j\}$ and we get $\mathrm{sgn}(d_{r(k)j}) = -\mathrm{sgn}(d_{kj})$. For each $d_k \in \mathcal{T}_j$, we get $d_{ik} \times d_{kj} = d_{ir(k)} \times d_{r(k)j}$ by Lemma 3.3 (5). Therefore, we have

$$B_{ij} = \sum_{k=1}^{s} \mathrm{sgn}(d_{kj})(d_{ik} \times d_{kj}) = \sum_{d_k \in \mathcal{T}_j} \mathrm{sgn}(d_{kj}) \left[(d_{ik} \times d_{kj}) - (d_{ir(k)} \times d_{r(k)j}) \right] = 0.$$

□

The matrix form of $C_{M,N}$ in the set S_2 on [10, P. 34] is then

$$\text{for } 1 \leq a \leq s, \quad (C_{M,N})_{a1} = \begin{cases} (-1)^{\omega(d_a)} = (-1)^n \times \mathrm{sgn}(d_a) & \text{if } \; d_a \mid M, \\ \qquad 0 & \text{otherwise.} \end{cases}$$

Finally, we prove the following lemma.

Lemma 3.6. *Let $E := \Lambda^{-1} C_{M,N}$. Then for $1 \leq a \leq s$ we have*

$$E_{a1} = \mathrm{sgn}(d_{s+1-a}) \times \frac{24}{\varphi(N)\psi(N/M)} \times \frac{d_{s+1-a}}{(d_{s+1-a},\; M)}.$$

In particular, $E_{s1} = (-1)^{\omega(N)} \frac{24}{\varphi(N)\psi(N/M)}$. Moreover if $M = N$, then we get

$$E_{a1} = \mathrm{sgn}(d_{s+1-a}) \times \frac{24}{\varphi(N)}.$$

Proof. Let $D := d_{s+1-a} = N/d_a$ and $E := (D,\, M)$. Then, by direct calculation we have

$$d_{ar} = d_a \boxplus d_r = \frac{D \times d_r}{(D,\, d_r)^2}$$

and the sign of $(\Lambda^{-1})_{ak} \times (C_{M,N})_{k1}$ is $\mathrm{sgn}(d_a) \times \mathrm{sgn}(d_k) \times (-1)^n \times \mathrm{sgn}(d_k) = \mathrm{sgn}(D)$ for any divisor d_k of M. Therefore we have

$$\begin{aligned} \sum_{k=1}^{s} \mathrm{sgn}(d_{ak}) \times d_{ak} \times (C_{M,\,N})_{k1} &= \mathrm{sgn}(D) \times \sum_{d_r \mid M} \frac{D \times d_r}{(D,\, d_r)^2} \\ &= \mathrm{sgn}(D) \times \frac{D}{E} \times \sum_{d_r \mid M} \frac{E \times d_r}{(E,\, d_r)^2}. \end{aligned}$$

We denote by

$$D_r := \frac{E \times d_r}{(E,\, d_r)^2} = \frac{(D,\, M) \times d_r}{((D,\, M),\, d_r)^2}.$$

Then, D_r is a divisor of M and for two distinct divisors $d_{r_1},\ d_{r_2}$ of M, we get $D_{r_1} \neq D_{r_2}$. Therefore, we have

$$\sum_{d_r | M} \frac{E \times d_r}{(E,\, d_r)^2} = \sum_{d_r | M} D_r = \sum_{d|M} d = \psi(M),$$

which implies the result. □

Now we give a proof of the theorem above.

Proof of Theorem 3.1. We check the conditions in Proposition 1 in *op. cit.* (We use the same notations.)

- The condition (0) implies that the order of $C_{M,N}$ is of the form $\frac{\varphi(N)\psi(N/M)}{24} \times g$ for some integer $g \geq 1$.
- The condition (1) always holds unless $M = N$ because $\sum_{\delta|N} r_\delta \cdot \delta = 0$. If $M = N$, then $\sum_{\delta|N} r_\delta \cdot \delta = (-1)^n g\varphi(N) \equiv 0 \pmod{24}$.
- The condition (2) implies that $g = \mathrm{num}(\frac{24}{\varphi(N)\psi(N/M)}) \times h$ for some integer $h \geq 1$ because $\sum_{\delta|N} r_\delta \cdot N/\delta = g\varphi(N)\psi(N/M) \equiv 0 \pmod{24}$.
- The condition (3) always holds.
- The condition (4) always holds unless M is a prime because $\prod_{\delta|N} \delta^{r_\delta} = 1$. If M is a prime, then it implies that $g\varphi(N/M)$ is even because $\prod_{\delta|N} \delta^{r_\delta} = M^{-g\varphi(N/M)}$.

In conclusion, the order of $C_{M,N}$ is equal to $\mathrm{num}(\frac{\varphi(N)\psi(N/M)}{24}) \times h$ for the smallest positive integer h satisfying all the conditions above. Therefore we get $h = 1$ unless all the following conditions hold:

(1) M is a prime;
(2) $\varphi(N/M) = 1$;
(3) $\mathrm{num}(\frac{24}{\varphi(N)\psi(N/M)})$ is odd.

Moreover if all the conditions above hold, then $h = 2$. By the first condition, M is a prime. By the second condition, either $N = M$ or $N = 2M$.

- Assume that $N = M$ is a prime greater than 3. Then, $h = 2$ if and only if $M \equiv 1 \pmod 8$. This is proved by Ogg [14].
- Assume that $N = 2M$. Then, $h = 2$ if and only if $M \equiv 1 \pmod 8$. This is proved by Chua and Ling [1].

□

4. Eisenstein series

As before, let $N = \prod_{i=1}^n p_i$ and $M = \prod_{i=1}^m p_i$ for $1 \leq m \leq n$. Let

$$e(z) := 1 - 24 \sum_{n \geq 1} \sigma(n) \times q^n$$

be the q-expansion of *Eisenstein series of weight* 2 of level 1 as on [12, p. 78], where $\sigma(n) = \sum_{d|n} d$ and $q = e^{2\pi i z}$.

Definition 4.1. For any modular form g of weight k and level A; and a prime p not dividing A, we define modular forms $[p]_k^+(g)$ and $[p]_k^-(g)$ of weight k and level pA by

$$[p]_k^+(g)(z) := g(z) - p^{k-1}g(pz) \quad \text{and} \quad [p]_k^-(g)(z) := g(z) - g(pz).$$

Using these operators, we define Eisenstein series of weight 2 and level N by

$$\mathcal{E}_{M,N}(z) := [p_n]_2^- \circ \cdots \circ [p_{m+1}]_2^- \circ [p_m]_2^+ \circ \cdots \circ [p_1]_2^+(e)(z).$$

(Note that $\mathcal{E}_{M,N} = -24E_{M,N}$, where $E_{M,N}$ is a normalized Eisenstein series in [21, §2.2].)

By Proposition 2.6 of *op. cit.*, we know that $\mathcal{E}_{M,N}$ is an eigenform for all Hecke operators and $I_{M,N}$ annihilates $\mathcal{E}_{M,N}$. By Proposition 2.10 of *op. cit.*, we can compute the residues of $\mathcal{E}_{M,N}$ at various cusps.

Proposition 4.2. *We have*

$$\mathrm{Res}_{P_N}(\mathcal{E}_{M,N}) = \begin{cases} (-1)^n \varphi(N) & \text{if } M = N, \\ 0 & \text{otherwise}. \end{cases}$$

Moreover, for a prime divisor p of N we have

$$\mathrm{Res}_{P_{N/p}}(\mathcal{E}_{N,N}) = (-1)^{n-1}\varphi(N) \quad \text{and} \quad \mathrm{Res}_{P_M}(\mathcal{E}_{M,N}) = (-1)^{\omega(M)}\varphi(N)\psi(N/M)(M/N).$$

Proof. The first statement follows from the definition (cf. [12, §II.5]). For the second statement, we use the method of Deligne-Rapoport [3] (cf. 3.17 and 3.18 in §VII.3) or of Faltings-Jordan [6] (cf. Proposition 3.34). Therefore the residue of $\mathcal{E}_{M,N}$ at P_1 is $\varphi(N)\psi(N/M)(M/N)$ (cf. [21, Proposition 2.11]). Since the Atkin-Lehner operator w_p acts by -1 on $\mathcal{E}_{M,N}$ for a prime divisor p of M, w_M acts by $(-1)^{\omega(M)}$ and hence the result follows. □

5. The index of an Eisenstein ideal

As before, let $N = \prod_{i=1}^n p_i$ and $M = \prod_{i=1}^m p_i$ for some $1 \leq m \leq n$. Let $\mathbb{T} := \mathbb{T}(N)$.

Note that $\mathbb{T}/I_{M,N} \simeq \mathbb{Z}/t\mathbb{Z}$ for some integer $t \geq 1$ [21, Lemma 3.1]. We compute the number t as precise as possible.

Theorem 5.1. *The index of $I_{N,N}$ is equal to the order of $C_{N,N}$ up to powers of 2.*

Theorem 5.2. *If $M \neq N$ and N/M is odd (resp. even), then the index of $I_{M,N}$ and the order of $C_{M,N}$ coincide (resp. coincide up to powers of 2).*

Before starting to prove the theorems, we introduce some notations.

Definition 5.3. For a prime ℓ, we define $\alpha(\ell)$ and $\beta(\ell)$ as follows:

$$(\mathbb{T}/I_{M,N}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z} \quad \text{and}$$

$$\ell^{\beta(\ell)} \text{ is the exact power of } \ell \text{ dividing num}\left(\frac{\varphi(N)\psi(N/M)}{24} \times h\right),$$

where h is the number in Theorem 3.1.

Since $I_{M,N}$ annihilates $C_{M,N}$, we get $\alpha(\ell) \geq \beta(\ell)$ (cf. [21, proof of Theorem 3.2]). Therefore to prove Theorems 5.1 and 5.2, it suffices to show that $\alpha(\ell) \leq \beta(\ell)$ for all (or odd) primes ℓ. If $\alpha(\ell) = 0$, then there is nothing to prove. Thus, we now assume that $\alpha(\ell) \geq 1$. Let

$$\mathcal{I} := (\ell^{\alpha(\ell)},\ I_{M,N})$$

and let δ be a cusp form of weight 2 and level N over the ring $\mathbb{T}/\mathcal{I} \simeq \mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z}$ whose q-expansion (at P_N) is

$$\sum_{n\geq 1} (T_n \bmod \mathcal{I}) \times q^n.$$

Now we prove the theorems above.

Proof of Theorem 5.1. First, let $\ell = 3$ and $M = N$. Let $E := \mathcal{E}_{N,N} \pmod{3^{\alpha(3)+1}}$ and $A = (-1)^{\omega(N)}\varphi(N)$. Since 24δ is a cusp form of weight 2 modulo $3^{\alpha(3)+1}$ (cf. [12, p. 86]), $E + 24\delta$ is a modular form of weight 2 and level N over $\mathbb{Z}/3^{\alpha(3)+1}\mathbb{Z}$. Let $a = \min\{\alpha(3),\ \beta(3)+1\}$. Then, by the q-expansion principle [8, §1.6] we have

$$E + 24\delta \equiv Ae \pmod{3^{a+1}}$$

on the irreducible component C of $X_0(N)_{\mathbb{F}_\ell}$ containing P_N because Ae is a modular form of weight 2 over $\mathbb{Z}/(12A)\mathbb{Z}$ and $(3^{\alpha(3)+1},\ 12A) = 3^{a+1}$. By the following lemma, we get $A \equiv 0 \pmod 3$ and hence we can choose a prime divisor p of N congruent to 1 modulo 3. Note that the cusp $P_{N/p}$ belongs to C. By Proposition 4.2, $\mathrm{Res}_{P_{N/p}}(E) = -A$ and $\mathrm{Res}_{P_{N/p}}(Ae) \equiv pA \pmod{12A}$ by Sublemma on [12, p. 86]. Combining all the computations above, we have

$$\mathrm{Res}_{P_{N/p}}(8\delta) \equiv \frac{(p+1)A}{3} \pmod{3^a}.$$

Since δ is a cusp form modulo $3^{\alpha(3)}$, we get $\mathrm{Res}_{P_{N/p}}(8\delta) \equiv 0 \pmod{3^{\alpha(3)}}$ and hence $3^{\beta(3)} \equiv 0 \pmod{3^{\alpha(3)}}$. In other words, we get $\alpha(3) \leq \beta(3)$.

Next, let $\ell \geq 5$ and $M = N$. Let $F := \mathcal{E}_{N,N} \pmod{\ell^{\alpha(\ell)}}$. Then, $f := F + 24\delta$ is a modular form of weight 2 and level N over $\mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z}$ whose q-expansion is A. Basically the inequality $\alpha(\ell) \leq \beta(\ell)$ follows from the non-existence of a mod ℓ modular form of weight 2 and leven N whose q-expansion is a non-zero constant (cf. [12, chap. II, Proposition 5.6] and [13, Proposition (2.2.6)]).

- If $\ell \nmid N$, then by Ohta [13, Lemma (2.1.1)], we can find a modular form g of weight 2 and level 1 such that $f(z) = g(Nz)$. Therefore $A \equiv 0 \pmod{\ell^{\alpha(\ell)}}$ (cf. [12, chap. II, Proposition 5.6]) and hence we get $\alpha(\ell) \leq \beta(\ell)$.
- Assume that $\ell \mid N$ and $\mathfrak{m} := (\ell, \mathcal{I})$ is not ℓ-new. Then, the argument basically follows from the previous case because the exact powers of ℓ dividing A and $\varphi(N/\ell)$ coincide. (For more detailed argument on lowering the level when $\ell \geq 5$, see the proof of Theorem 5.2 below.)
- Assume that $\ell \mid N$ and $\mathfrak{m} := (\ell, \mathcal{I})$ is ℓ-new. Then, we can lift δ to a modular form $\widetilde{\delta}$ of weight 2 and level N over $\mathbb{Z}_{(\ell)}$ satisfying $w_\ell(\widetilde{\delta}) = -\widetilde{\delta}$, where $\mathbb{Z}_{(\ell)}$ is the localization of $\mathbb{Z}$ at ℓ. Therefore $\widetilde{\delta}$ determines a regular differential on $X_0(N)_{\mathbb{Z}_{(\ell)}}$ over $\mathbb{Z}_{(\ell)}$ (cf. [13, Proposition (1.4.9)]). Similarly, we can lift F to $\mathcal{E}_{N,N}$ as well and $w_\ell(\mathcal{E}_{N,N}) = -\mathcal{E}_{N,N}$. Therefore $f = \mathcal{E}_{N,N} + 24\widetilde{\delta} \pmod{\ell^{\alpha(\ell)}}$ can be regarded as a regular differential on $X_0(N)_{\mathbb{Z}_{(\ell)}}$ over $\mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z}$ whose q-expansion is A. If $\alpha(\ell) \geq \beta(\ell)+1$, then $g = f \pmod{\ell^{\beta(\ell)+1}}$ is a regular differential over $\mathbb{Z}/\ell^{\beta(\ell)+1}\mathbb{Z}$. Moreover $\ell^{-\beta(\ell)} \times g$ can be regarded as a regular differential over $\mathbb{F}_\ell$ whose q-expansion is a non-zero constant (cf. [12, p. 86]), which is a contradiction (cf. [13, Proposition (2.2.6)]). Thus, we get $\alpha(\ell) \leq \beta(\ell)$.

□

Lemma 5.4. *If $\mathfrak{m} := (3, I_{N,N})$ is maximal, then $A = (-1)^{\omega(N)}\varphi(N) \equiv 0 \pmod 3$.*

Proof. As above, let $E := \mathcal{E}_{N,N} \pmod 9$ and $\eta := \delta \pmod{\mathfrak{m}}$. Let $f := E + 24\eta$ be a modular form of weight 2 and level N over $\mathbb{Z}/9\mathbb{Z}$ whose q-expansion is A.

First, assume that 3 does not divide N. Then by Ohta [13, Lemma (2.1.1)], we can find a modular form g of weight 2 and level 1 over $\mathbb{Z}/9\mathbb{Z}$ such that $f(z) = g(Nz)$. By Mazur [12, chap. II, Proposition 5.6], we get $A \equiv 0 \pmod 3$.

Next, assume that $p_1 = 3$ and $N = 3M$. If $\mathfrak{m}$ is 3-old, then the result follows from the previous case. Thus, we further assume that $\mathfrak{m}$ is 3-new. Then as above, we can regard η as a regular differential on $X_0(N)_{\mathbb{Z}_{(\ell)}}$ over $\mathbb{F}_3$ and hence there is a modular form ζ of weight $3+1$ and level M over $\mathbb{F}_3$ which has the same q-expansion as η by Ohta [13, Proposition (2.2.4)]. By the same argument as on [12, p. 86], 240ζ is a modular form of weight 4 and level M over $\mathbb{Z}/9\mathbb{Z}$. Let E_4 be the usual Eisenstein series of weight 4 and level 1:

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) \times q^n,$$

where $\sigma_3(n) = \sum_{d \mid n} d^3$ and $q = e^{2\pi i z}$. Let $G(z) := [p_n]_4^+ \circ \cdots \circ [p_2]_4^+(E_4)(z)$ be an Eisenstein series of weight 4 and level M whose constant term is $\prod_{i=2}^n (1-p_i^3)$. Now we consider the modular form $h := G \pmod 9 - 240\zeta$ of weight 4 and level M over $\mathbb{Z}/9\mathbb{Z}$. Since the q-expansion of h is $\prod_{i=2}^n (1-p_i^3)$, there is a modular form H of weight 4 and level 1 over $\mathbb{Z}/9\mathbb{Z}$ such that $h(z) = H(Mz)$ by Ohta [13, Lemma (2.1.1)]. However if $A \not\equiv 0 \pmod 3$, then there is no such a modular form over $\mathbb{Z}/9\mathbb{Z}$ (cf. [13, p. 308]) because $1 - p_i^3 \equiv 1 - p_i \pmod 3$. Therefore we get $A \equiv 0 \pmod 3$. □

Proof of Theorem 5.2. Since we assume that $\alpha(\ell) \geq 1$, $\mathfrak{m} := (\ell, I_{M,N})$ is maximal.

First, assume that N/M is divisible by an odd prime ℓ. Then $U_\ell \equiv \ell \equiv 0 \pmod{\mathfrak{m}}$ and hence $\mathfrak{m}$ is not ℓ-new. Thus, we get $\mathbb{T}(N)/\mathcal{I} \simeq \mathbb{T}(N)^{\ell\text{-old}}/\mathcal{I}$. Let R be the common subring of $\mathbb{T}(N/\ell)$ and $\mathbb{T}(N)^{\ell\text{-old}}$, which is generated by all T_n with $\ell \nmid n$. Then, as in the proof of Lemma 2.1, $\mathbb{T}(N/\ell) = R[T_\ell]$ and $\mathbb{T}(N)^{\ell\text{-old}} = R[U_\ell]$. Note that if ℓ is odd then $R = \mathbb{T}(N/\ell)$ by Ribet [20, p. 491] and $\mathbb{T}(N)^{\ell\text{-old}} \simeq R[X]/(X^2 - T_\ell X + \ell)$. Let I be the ideal of R generated by all the generators of $\mathcal{I}$ but $U_\ell - \ell$. Then, we show that $T_\ell - \ell - 1 \in I$ as follows. Note

that the kernel K of the composition of the maps

$$R = \mathbb{T}(N/\ell) \hookrightarrow \mathbb{T}(N)^{\ell\text{-old}} = R[U_\ell]/(U_\ell^2 - T_\ell U_\ell + \ell) \twoheadrightarrow \mathbb{T}(N)^{\ell\text{-old}}/\mathcal{I} \simeq \mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z}$$

(sending T_n to $T_n \pmod{\mathcal{I}}$) is $(I,\ \ell(T_\ell - \ell - 1))$ and this composition is clearly surjective. Thus, we get $R/I \twoheadrightarrow R/K$. Since all the generators of R are congruent to integers modulo I; and I contains $\ell^{\alpha(\ell)}$, we have $R/I = R/K \simeq \mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z}$; in particular $\ell(T_\ell - \ell - 1) \in I$. Let f be a cusp form over R/I whose q-expansion is $\sum_{n\geq 1}(T_n \bmod I) \times q^n$.

- Suppose that $\ell \geq 5$. Let $E := \mathcal{E}_{M,\,N/\ell} \pmod{\ell^{\alpha(\ell)}}$ and let $g := 24f + E$. Then, g is a modular form over $R/I \simeq \mathbb{Z}/\ell^{\alpha(\ell)}\mathbb{Z}$ whose q-expansion is of the form $\sum_{k\geq 0} a_k \times q^{\ell k}$. By Katz [9, Corollaries (2) and (3) of the main theorem], we get $g = 0$ and hence $a_1/24 = T_\ell - \ell - 1 \in I$. (Note that the constant term a_0 must be 0 and hence we get $\alpha(\ell) \leq \beta(\ell)$ as well if $M = N/\ell$.)
- Suppose that $\ell = 3$. Let $E := \mathcal{E}_{M,\,N/\ell} \pmod{3^{\alpha(3)+1}}$ and let $g := 24f + E$. Then, g is a modular form over $\mathbb{Z}/3^{\alpha(3)+1}\mathbb{Z}$ whose q-expansion is of the form $\sum_{k\geq 0} a_k \times q^{\ell k}$. If $a_1 = 0 \in \mathbb{Z}/3^{\alpha(3)+1}\mathbb{Z}$ then $a_1/24 = T_3 - 4 = 0 \in \mathbb{Z}/3^{\alpha(3)}\mathbb{Z} \simeq R/I$ and hence $T_3 - 4 \in I$. Therefore it suffices to show that $a_1 = 0 \in \mathbb{Z}/3^{\alpha(3)+1}\mathbb{Z}$.

  If $M \neq N/\ell$ then $a_0 = 0$ and hence $g = 0$ by Corollaries (3) and (4) in *loc. cit.* Therefore $a_1 = 0$.

  Suppose that $M = N/\ell$. Then, $a_0 = (-1)^{\omega(M)}\varphi(M)$. Note that the exact power of 3 dividing a_0 is $3^{\beta(3)+1}$. Since $3(T_3 - 4) \in I$, $g \pmod{3^{\alpha(3)}}$ is a modular form over $\mathbb{Z}/3^{\alpha(3)}\mathbb{Z}$ whose q-expansion is a constant a_0. Since $a_0 \times e$ is a modular form over $\mathbb{Z}/3^{\beta(3)+2}\mathbb{Z}$ whose q-expansion is a_0, by the q-expansion principle $g = 24f + E \equiv a_0 \times e \pmod{3^a}$, where $a = \min\{\alpha(3),\ \beta(3)+2\}$. Since $\mathfrak{m}$ is ℓ-old, there is the corresponding maximal ideal $\mathfrak{n}$ of $\mathbb{T}(N/\ell)$ to $\mathfrak{m}$. Hence by Lemma 5.4, $a_0 \equiv 0 \pmod{3}$ and we can find a prime divisor p of N/ℓ such that $p \equiv 1 \pmod{3}$. By comparing the residues of g and $a_0 \times e$ at $P_{N/p}$ as in the proof of Theorem 5.1, we get $(p+1)a_0 \equiv 0 \pmod{3^a}$ and hence $\alpha(3) \leq \beta(3) + 1$. Therefore $h := 3^{-\alpha(3)} \times g$ is a modular form over $\mathbb{F}_3$. Again by Corollary (5) in *loc. cit.* and by Mazur [12, Proposition 5.6 (b)], we get $h = 3^{-\alpha(3)} \times a_0 \times e$; in particular, $3^{-\alpha(3)} \times a_1 \equiv 0 \pmod{3}$, i.e., $a_1 = 0 \in \mathbb{Z}/3^{\alpha(3)+1}\mathbb{Z}$ as desired.

(Note that in the first case, we can allow the case where $M = N$ by taking $E := \mathcal{E}_{M/\ell,N/\ell} \pmod{\ell^{\alpha(\ell)}}$, which is used in the proof of Theorem 5.1 above.) Therefore we have $I = (\ell^{\alpha(\ell)},\ I_{M,N/\ell})$ and

$$\mathbb{T}(N)/\mathcal{I} \simeq \mathbb{T}(N)^{\ell\text{-old}}/\mathcal{I} \simeq R/I = \mathbb{T}(N/\ell)/(\ell^{\alpha(\ell)},\ I_{M,N/\ell}).$$

Accordingly, it suffices to prove that $\alpha(\ell) \leq \beta(\ell)$ for primes ℓ not dividing N/M because $\ell \nmid \ell^2 - 1$.

Next, we assume that ℓ does not divide N/M. Let $F := \mathcal{E}_{M,N} \pmod{24\ell^{\alpha(\ell)}}$ and δ be a cusp form as above. Since F and -24δ have the same q-expansions (at P_N), they coincide on the irreducible component D of $X_0(N)_{\mathbb{F}_\ell}$, which contains P_N. Note that the cusp P_M belongs to D because $\ell \nmid N/M$. Since -24δ is a cusp form over the ring $\mathbb{Z}/24\ell^{\alpha(\ell)}\mathbb{Z}$, the residue of F at P_M must be zero. By Proposition 4.2, $\varphi(N)\psi(N/M)(M/N) \equiv 0 \pmod{24\ell^{\alpha(\ell)}}$. Therefore we get $\alpha(\ell) \leq \beta(\ell)$. (Note that if $\ell = 2$, then $h = 1$ with the assumption that $M \neq N$ and $\ell \nmid N/M$.) □

If ℓ is odd and $\ell \nmid \varphi(N)$, we prove the following.

Proposition 5.5. *Let ℓ be an odd prime and $\mathfrak{m} := (\ell,\ I_{1,N})$. Hence, we assume that $\ell \nmid \varphi(N)$ from the definition (cf. §2). Then, $\mathfrak{m}$ cannot be maximal.*

Proof. Assume that $\mathfrak{m}$ is maximal. If $\ell \mid N$, then $\mathfrak{m}$ cannot be ℓ-new because $U_\ell \equiv \ell \equiv 0 \pmod{\mathfrak{m}}$. Therefore there is a maximal ideal $\mathfrak{n} := (\ell,\ I_{1,N/\ell})$ in the Hecke ring $\mathbb{T}(N/\ell)$ of level N/ℓ. Thus, we may assume that $\ell \nmid N$. Then as above, δ is a mod ℓ cusp form of weight 2 and level N. Let $g = \mathcal{E}_{N,N} \pmod{24\ell} + 24\delta$ be a modular form over $\mathbb{Z}/24\ell\mathbb{Z}$.

First, consider the case where $n = \omega(N) = 1$.

- If $\ell \geq 5$, then g is a mod ℓ modular form of weight 2 and level N as above. Since the q-expansion of g is

$$(1 - N) + 24(1 - N)\sum_{i=1}^{\infty} \sigma(d) \times q^{dN},$$

we get $\frac{g}{1-N}=0$ by Mazur [12, chap. II, Corollary 5.11], which is a contradiction. Therefore $\mathfrak{m}$ is not maximal.

- If $\ell=3$, then g is a modular form of weight 2 and level N over $\mathbb{Z}/9\mathbb{Z}$ as above. Then, by Mazur [12, chap. II, Lemma 5.9], there is a modular form G of level 1 over $\mathbb{Z}/9\mathbb{Z}$ such that $G(Nz)=\frac{g(z)}{1-N}$. However this contradicts Proposition 5.6(c) in [12, chap. II]. Therefore $\mathfrak{m}$ is not maximal.

Next, consider the case where $n\geq 2$. Let $F_N(q):=(-1/24)\times\mathcal{E}_{1,N}\in\mathbb{Z}[[q]]$ be a formal q-expansion. Since $\mathfrak{m}$ is maximal, $\delta\equiv F_N(q) \pmod{\ell}$ is a mod ℓ modular form of weight 2 and level N. Then, by the following lemma, we can lower the level of δ because $\varphi(N)\not\equiv 0 \pmod{\ell}$. Therefore the result follows from the case where $n=1$. □

Lemma 5.6. *Let $N=pD$ be a square-free integer with $D>1$ and p a prime. Assume that $p\not\equiv 1 \pmod{\ell}$ and $\ell\nmid N$. Let $F_N(q):=(-1/24)\times\mathcal{E}_{1,N}\in\mathbb{Z}[[q]]$ be a formal q-expansion. If $F_N(q) \pmod{\ell}$ is the q-expansion of a mod ℓ modular form of weight 2 and level N, then $F_D(q) \pmod{\ell}$ is also the q-expansion of a mod ℓ modular form of weight 2 and level D.*

Proof. Let $G(q):=(-1/24)\times\mathcal{E}_{p,N}$. Then, as formal q-expansions we get

$$F_N(q)-G(q)=(p-1)F_D(q^p).$$

Therefore if $F_N(q) \pmod{\ell}$ is the q-expansion of a mod ℓ modular form of level N, then there is a mod ℓ modular form of level D whose q-expansion is $(p-1)F_D(q) \pmod{\ell}$ by Ohta [13, Lemma (2.1.1)]. Therefore the result follows because $p\not\equiv 1 \pmod{\ell}$. □

6. Proof of the main theorem

In this section, we prove our main theorem.

Theorem 6.1. *Let $\mathfrak{m}:=(\ell,\ I_{M,N})$ be a maximal ideal of $\mathbb{T}(N)$. Then $\mathcal{C}_N[\mathfrak{m}]\neq 0$.*

Proof. If ℓ is odd, then the result follows from Theorems 5.1 and 5.2. Therefore we assume that $\ell=2$. By the definition of the notation, M is either N or $N/2$.

- If N is a prime and $N=M$, then $M\equiv 1 \pmod 8$ by Mazur [12]. Thus, we have $\mathcal{C}_N[\mathfrak{m}]\neq 0$.
- If N is not a prime and $N=M$, then we set $N=pD$ with D odd and $\omega(D)\geq 1$. (In other words, if N is even then we set $p=2$.) Since $(2,\ I_{N,N})=(2,\ I_{p,N})$ is maximal, the index of $I_{p,N}$, which is equal to the order of $C_{p,N}$, is divisible by 2 and hence $\langle C_{p,N}\rangle[\mathfrak{m}]\neq 0$, which implies that $\mathcal{C}_N[\mathfrak{m}]\neq 0$.
- If $N=2M$ with $\omega(M)=1$, then $\mathfrak{m}$ is not 2-new and hence there is the corresponding Eisenstein maximal ideal of $\mathbb{T}(M)$. Therefore $M\equiv 1 \pmod 8$ by Mazur. This implies that the order of $C_{M,N}$ is $\frac{M-1}{4}$ by Theorem 3.1. Thus, we get $\mathcal{C}_N[\mathfrak{m}]\neq 0$.
- If $N=2M$ with $\omega(M)\geq 2$, then the order of $C_{p,N}$ is divisible by 2, where p is any prime divisor of M. Therefore we get $\mathcal{C}_N[\mathfrak{m}]\neq 0$.

□

References

[1] Seng-Kiat Chua and San Ling, *On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$*, Proc. Amer. Math. Soc., Vol **125**, Number **8** (1997), 2255–2263.

[2] Henry Darmon and Fred Diamond and Richard Taylor, *Fermat's Last Theorem*, Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993), International press, Cambridge (1995), 2–140.

[3] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable II, Lecture notes in Math., Vol. **349** (1973), 143–316.

[4] Vladimir Drinfeld, *Two theorems on modular curves*, Functional Anal. Appl. **7** (1973), 155–156.

[5] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), 563–594.

[6] Gerd Faltings and Bruce Jordan, *Crystalline cohomology and* $\mathrm{GL}(2,\mathbb{Q})$, Israel Journal of Math., Vol **90**. (1995), 1–66.

[7] Günter Harder, *Eisenstein cohomology and the construction of mixed motives*, preprint, available at http://www.math.uni-bonn.de/people/harder/Manuscripts/Eisenstein/Mix-Mot-2015.pdf (2015).

[8] Nicholas Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable III, Lecture notes in Math., Vol. **350** (1973), 69–190.

[9] Nicholas Katz, *A result on modular forms in characteristic p*, Modular functions of one variable V, Lecture notes in Math., Vol. **601** (1976), 53–61.

[10] San Ling, *On the $\mathbb{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$*, Israel Journal of Math., Vol **99** (1997), 29–54.

[11] Yuri Manin, *Parabolic points and zeta functions of modular curves (in Russian)*, Izv. Akad. Nauk SSSR Ser. Mat., **36**, 19–66 (1972). Translation in Math USSR-Izv **6** (1972), 19-64.

[12] Barry Mazur, *Modular curves and the Eisenstein Ideal*, Publications Math. de l'I.H.É.S., tome **47** (1977), 33–186.

[13] Masami Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo Journal of Math., Vol. **37**, no. 2 (2014), 273–318.

[14] Andrew Ogg, *Rational points on certain elliptic modular curves*, Proc. Sympos. Pure Math., vol. **24**, AMS, Providence, R. I. (1973), 221–231.

[15] Andrew Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France, Vol. **102** (1974), 449–462.

[16] Kenneth Ribet, *Congruence relations between modular forms*, Proceeding of the International Congress of Math., Vol. **1**, **2** (Warsaw, 1983) (1983), 503–514.

[17] Kenneth Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100**, no. 2 (1990), 431–476.

[18] Kenneth Ribet, *Eisenstein primes for $J_0(pq)$*, unpublished (2008).

[19] Toshikazu Takagi, *The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free*, Journal of Algebra, Vol. **193** (1997), 180–213.

[20] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math., Vol. **141** (1995), 443–551.

[21] Hwajong Yoo, *The index of an Eisenstein ideal and multiplicity one*, submitted, available at http://arxiv.org/pdf/1311.5275.pdf (2014).

[22] Hwajong Yoo, *Non-optimal levels of a reducible mod ℓ modular representation*, submitted, available at http://arxiv.org/pdf/1409.8342.pdf (2014).

CENTER FOR GEOMETRY AND PHYSICS, INSTITUTE FOR BASIC SCIENCE (IBS), POHANG, REPUBLIC OF KOREA 37673

E-mail address: hwajong@gmail.com